PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-046560
(43)Date of publication of application : 26.02.1993

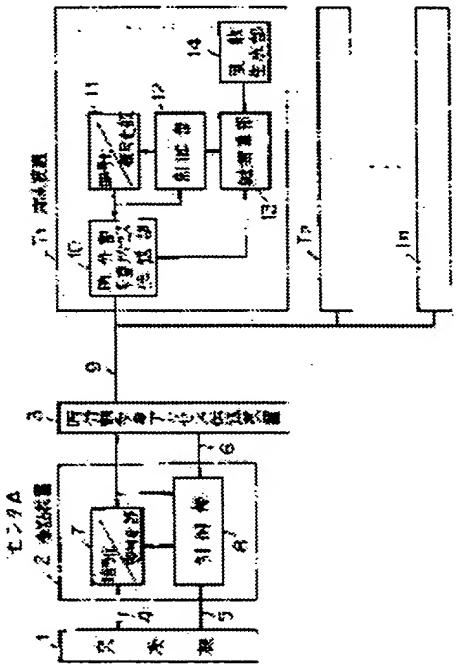
(51)Int.Cl. G06F 15/00
G06F 12/14

(21)Application number : 03-026401
(22)Date of filing : 20.02.1991

(71)Applicant : C EE T V KIBAN GIJUTSU KENKYUSHO:KK
(72)Inventor : TOTSUKA HISAYOSHI
SATO HAJIME

(54) SECRET KEY GENERATING SYSTEM

(57)Abstract:
PURPOSE: To grant the secret keys in a simple way without performing the key control in particular.
CONSTITUTION: When a power supply is turned on for registration of the terminals T1-Tn at 8 center A, a random number generating part 1.4 starts to apply the polling to each terminal through the center A and then to assign the time slots so that the UP signals received from the terminals never overlap each other. Therefore the delay measurement control is applied to each terminal. Then the random number value of the part 14 obtained at each terminal when the delay measurement control is complete is defined as a secret key of the relevant terminal. The different types of delay measurement control are always applied to the terminals T1-Tn respectively and therefore the secret keys are proper to each terminal. Based on these secret keys, the open keys and the shared keys are computed at a key computing part 13. The open keys are sent to the center A, and the shared keys are produced from the open keys at the center A.



LEGAL STATUS

[Date of request for examination]	20.02.1991
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2007679
[Date of registration]	11.01.1996
[Number of appeal against examiner's decision of rejection]	

[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right] 18.01.2003

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平5－46560

(43)公開日　平成５年(1993)２月26日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０　Ｅ	8219－5L		
	12/14	３２０　Ｂ	9293－5Ｂ		

審査請求　有　　請求項の数１(全　４　頁)

(21)出願番号　特願平3－26401

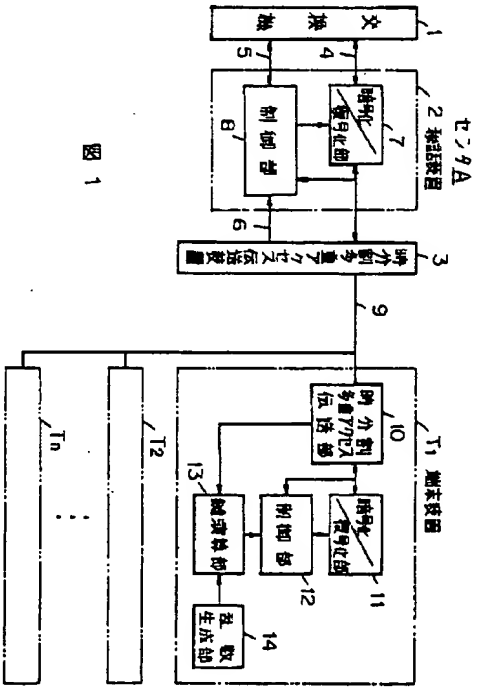
(22)出願日　平成３年(1991)２月20日

(71)出願人　591050039
株式会社シーエーテイブイ基盤技術研究所
東京都新宿区歌舞伎町１丁目２番３号
(72)発明者　戸塚　久義
東京都新宿区歌舞伎町１丁目２番３号　株式会社シーエーテイブイ基盤技術研究所内
(72)発明者　佐藤　肇
東京都新宿区歌舞伎町１丁目２番３号　株式会社シーエーテイブイ基盤技術研究所内
(74)代理人　弁理士　草野　卓

(54)【発明の名称】　秘密鍵生成方式

(57)【要約】
【目的】　秘密鍵の付与を、特に鍵管理を行うことなく簡単に行う。
【構成】　端末Ｔ１～Ｔｎがセンタ Ａに登録されるため、その電源をオンにすると、乱数生成部１４が起動し、センタより各端末に対し、ポーリングを行い、各端末からの上り信号が重ならないように、タイムスロットを割当るために、遅延計測制御が各端末に対して行われ、その遅延計測制御が終了すると、その時のその端末における乱数生成部１４の乱数値がその端末に対する秘密鍵とされる。各端末に対する遅延計測制御は必ず異ったものとなるから、この秘密鍵は、端末固有のものとなる。この秘密鍵をもとに、鍵演算部１３で公開鍵、共有鍵が演算され、公開鍵はセンタへ送られ、センタでその公開鍵から共有鍵が作られる。

図１



【特許請求の範囲】
【請求項１】　センター端末間で時分割多重アクセス伝送を行い、かつ端末ー端末間またはセンター端末間での音声やデータの秘密通信を行う際に、お互いにそれぞれ固有の秘密鍵を生成し、その秘密鍵から公開鍵を算出し、通信の前にお互いにその公開鍵の授受を行い、自分の秘密鍵と相手の公開鍵とより互いに共有の鍵を算出し、その共有鍵により音声やデータを暗号化・復号化する秘話通信システムにおいて、
各端末に乱数生成部を設け、
電源投入を契機として上記乱数生成部で乱数生成を開始し、
時分割多重アクセス伝送のための初期処理が完了した時点の乱数をその端末の上記秘密鍵とすることを特徴とした秘密鍵生成方式。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】この発明はセンター端末間で時分割多重アクセス伝送を行い、かつ端末ー端末間またはセンター端末間で音声やデータの秘密通信を行う際に、お互いに固有の秘密鍵を生成し、その秘密鍵から公開鍵を算出し、通信に先立ちその公開鍵を互いに授受し、自分の秘密鍵と相手の公開鍵とより互いに共有の鍵を算出し、その共有鍵を用いて音声やデータを暗号化、復合化する秘密通信システムにおける秘密鍵を生成する秘密鍵生成方式に関する。
【０００２】
【従来の技術】慣用暗号方式による暗号化は暗号鍵により行っており、鍵が異なれば復号できない。従って、端末毎に固有の暗号鍵等の設定が必要である。従来端末装置では暗号鍵そのものや秘密鍵が製作時にＩＣ等に作り込まれるか、またはＩＣカード等の外部機器によってセットされていた。
【０００３】
【発明が解決しようとする課題】このように従来の暗号鍵配送方式では、暗号鍵そのものまたは秘密鍵を製作時ＩＣ等に作り込むか、あるいはＩＣカード等の外部機器によってセットしていたため、端末と鍵との関係、鍵の設定・変更等の鍵管理が必要であったり、設定のための製作費や工事費が必要であった。
【０００４】この発明の目的はこのような課題を解決するためになされたもので、オペレータが暗号鍵を意識しないでシステムの運用ができ、製造業者、工事業者も暗号鍵を意識しないで製造・工事ができる秘密鍵生成方式を提供することにある。
【０００５】
【課題を解決するための手段】この発明はセンター端末間で時分割多重アクセス伝送通信システムを前提とする。時分割多重アクセス伝送方式ではセンタにおいて各端末装置からの上り信号のタイムスロットが衝突しないように、センター端末間での遅延計測制御を行い、端末での送出タイミングを指示する。この処理は端末装置の番号により順次行われることから、端末装置の電源が投入されてからその遅延計測が完了するまでの時間は端末固有の値となる。また、伝送路による損失が端末装置の設置位置によりそれぞれ異なるために端末出力レベルの制御が必要であり、このレベル計測制御も端末設置位置によりばらつきを持っている。これらの遅延計測制御、レベル計測制御などの初期処理が終了することにより、センター端末間の通信準備が出来、端末装置レディとなる。
【０００６】この発明では各端末装置に一定間隔で乱数を生成する乱数生成部を設け、端末装置では電源投入と同時にその乱数生成部を起動させ、その端末装置について時分割多重アクセス伝送のための前記初期処理が終了してレディになったときの乱数生成部よりの乱数を取り出し、その乱数をその端末固有の秘密鍵とする。
【０００７】
【作用】この発明によれば、端末装置がレディになればその端末に固有の秘密鍵が得られ、暗号鍵に関して、端末装置製造時、または設置時に固有の値をセットする必要がなく、オペレータ等による鍵管理も必要がない。
【０００８】
【実施例】以下、図１を参照して、この発明の一実施例を説明する。センタＡは交換機１、秘話装置２及び時分割多重アクセス伝送装置３から構成され、秘話装置２は暗号化／復号化部７及び制御部８から成る。端末装置Ｔ１～T_nはそれぞれ時分割多重アクセス伝送部１０、暗号化／復号化部１１、制御部１２、鍵演算部１３及び乱数生成部１４から成る。
【０００９】センタＡから端末装置T_1～T_nへの下り信号は時分割多重され、伝送路９にて各端末全てに伝送される。端末装置T_1～T_nからセンタＡへの上り通信では各端末の信号が衝突しないように遅延計測制御された時分割多重信号が、下り信号とは別の周波数を時分割多重アクセス伝送部１０で変調して、伝送路９にて伝達される。
【００１０】端末装置T_1～T_nがセンタＡの時分割多重アクセス伝送装置３に登録された時点から専用タイムスロットにて遅延計測制御、レベル計測制御がポーリングにより行われる。登録された端末装置T_1～T_nが網に接続され、電源投入されて遅延計測制御が終了する迄の時間は端末装置固有の値となる。また、レベル計測制御時間は端末の設置位置によっても収束時間のばらつきがあるため、全端末装置で同一の値にはならない。時分割多重アクセス伝送装置３はこの２つの条件が成立した時点で端末装置レディを専用タイムスロットを使って対応する端末装置に通知するとともに状態信号受信路６を使って秘話装置２にも通知する。
【００１１】端末装置T_1～T_nでその端末装置の電源

投入時から上記ポーリング周期より十分速い間隔で順次乱数を生成する乱数生成部１４を起動させ、センタＡの時分割多重アクセス伝送装置３からのレディ信号がオンになった時、その乱数生成部１４から取り出した乱数値をその端末の秘密鍵とする。演算部１３はその秘密鍵により公開鍵を算出し、更に予め設定されているセンタＡの公開鍵と前記秘密鍵とにより共有鍵を算出する。

【００１２】端末装置T_1～T_nにおいては制御部１２が暗号化／復号化部１１に上記共有鍵を指示し、暗号化／復号化部１１がセンタＡの交換機１からその端末に割り付けられた通信用のタイムスロットに対して上記共有鍵で暗号化／復号化を行う。秘話装置２は状態信号受信路６にて時分割多重アクセス伝送装置３から端末装置T_1～T_nのレディ信号を受けた後、その端末装置の公開鍵を収集するために公開鍵収集用のタイムスロットによりその端末装置に対して伝送路９を通して公開鍵送出要求を出力する。その端末装置においては公開鍵が既に算出されていて、秘話装置２から公開鍵送出要求がくれば、公開鍵収集用タイムスロットに鍵演算部１３に得られている公開鍵をのせて秘話装置２に送り出す。秘話装置２の制御部８においてはその端末装置からの公開鍵と予め設定されているセンタＡの秘密鍵とによりその端末装置との共有の鍵を算出する。

【００１３】秘話装置２の制御部８では交換機１にて通話用に割り付けられたセンター端末間のタイムスロットが制御データ授受信号路５にて交換機１から指示されるとそのタイムスロットと共有鍵を暗号化／復号化部７に指示する。暗号化／復号化部７では交換機１からデータ通信路４を通して送られてきた下りデータのそのタイムスロットに暗号化を行い、時分割多重アクセス伝送装置３から入力される端末装置T_1～T_nの上りデータのそのタイムスロットに対して復号化を行うことにより暗号通信を行う。

【００１４】

【発明の効果】以上説明したようにこの発明によれば時分割多重アクセス伝送のための初期処理が完了した時の乱数をその端末の秘密鍵とすることにより自動的に各端末に固有の秘密鍵が与えられ、暗号鍵管理が不要であり、かつ同一端末装置においてＩＣに各別の秘密鍵を作り込む必要もなく、単に同一の端末装置を作ればよく、製造及び設置工事の簡素化が可能となる。

【図面の簡単な説明】

【図１】この発明の一実施例を示すブロック図。

【図１】

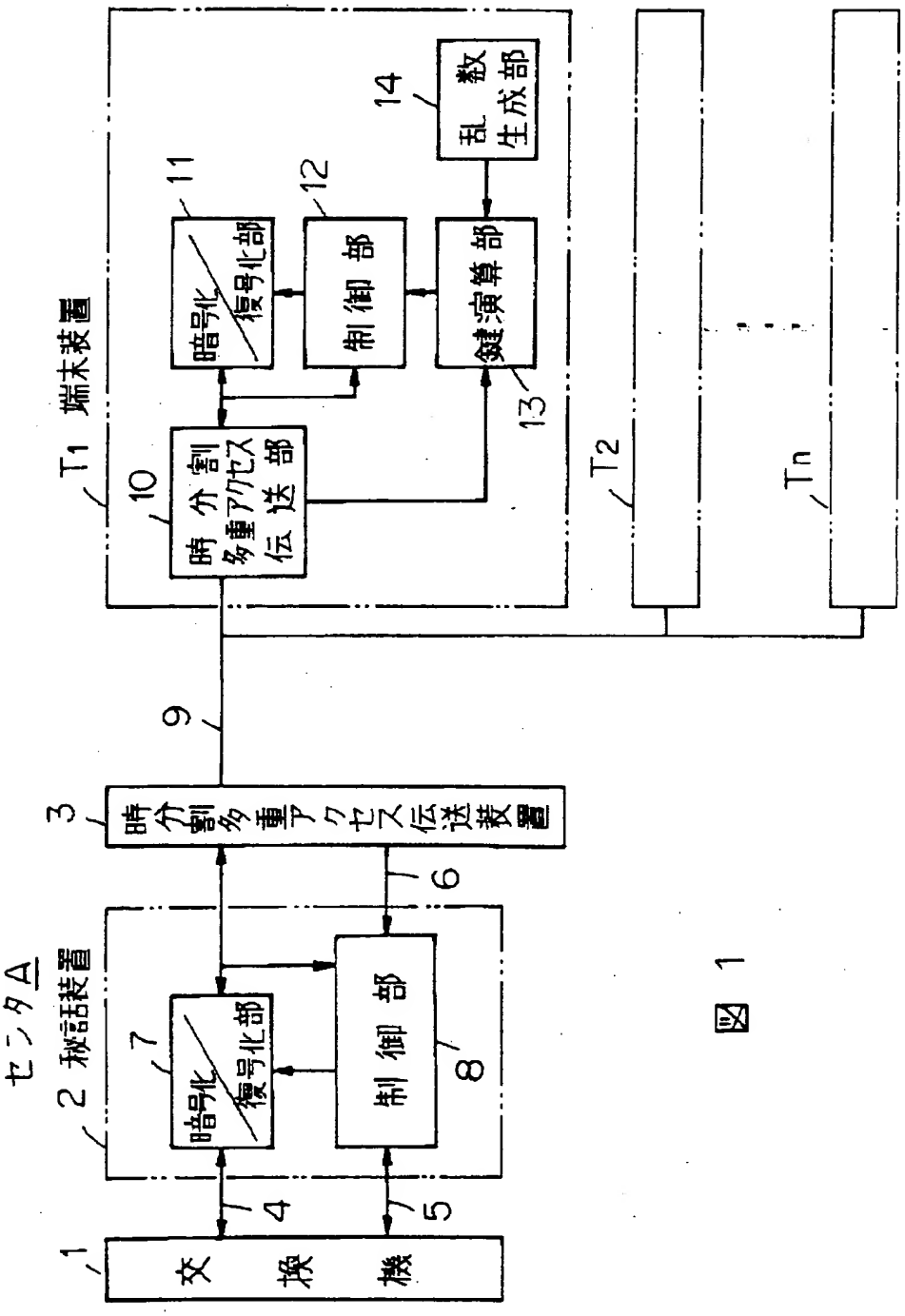

センタA
2 秘話装置
暗号化
復号化部
7
制御部
8
4
5
1
交換機
3
時分割多重アクセス伝送装置
9
6
T1 端末装置
時分割多重アクセス伝送部
10
暗号化
復号化部
11
制御部
12
鍵演算部
13
乱数生成部
14
T2
Tn

図１